EUROPEAN PATENT OFFICE

Patent Abstracts of Japan

PUBLICATION NUMBER : 03269756
PUBLICATION DATE : 02-12-91

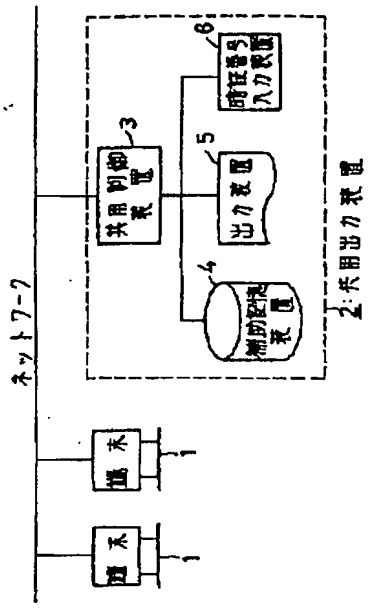
APPLICATION DATE : 20-03-90
APPLICATION NUMBER : 02070614

APPLICANT : FUJITSU LTD;

INVENTOR : ISHIGURO KEIJI;

INT.CL. : G06F 15/00 G06F 13/00

TITLE : SHARED OUTPUT DEVICE WITH SECURITY FUNCTION



ABSTRACT : PURPOSE: To use a shared output device to safely output secret data by temporarily preserving data with a password number, which is sent through a network, in the memory of the shared output device without outputting and outputting this data in response to input of the password number or the like.

CONSTITUTION: When data sent from a terminal 1 to a shared output device 2 through the network has the password number, this data is preserved in an auxiliary storage device 4; but otherwise, data is printed by an output device 5. When the user of the terminal 1 goes to the place of the shared output device 2 and inputs the password number number from a password number input device 6 to indicate the output, pertinent image data is taken out and is sent to the output device 5 and is printed if preserved in the auxiliary storage device 4. Thus, secret document is safely printed.

(11) Japanese Unexamined Patent Application Publication No. 3-269756

(43) Publication Date: December 2, 1991

(21) Application No. 2-70614

(22) Application Date: March 20, 1990

(71) Applicant: Fujitsu Ltd.

(72) Inventor: Keiji ISHIGURO

(74) Agent: Patent Attorney, Morihiro OKADA

SPECIFICATION

1. Title of the Invention: SHARED OUTPUT DEVICE HAVING SECURITY FUNCTION

2. Claim

A shared output device having a security function which outputs data from a shared output device to a network while keeping security thereof, wherein:

The shared output device (2) receives and once stores data with a password sent from a terminal (1) via the net work, and the corresponding stored data is fetched and outputted in response to the direct input of the password into said shared output device (2).

3. Detailed Description of the Invention

[Outline]

The present invention provides a shared output device having a security function which outputs data from the output device connected to a network while keeping security thereof, which has an object to:

Store once data having a password sent via the network, without outputting, in a memory in the shared output device, output the data in response to the input of the password or the like, and securely output the confidential data by the use of the shared output device which:

The shared output device receives and once stores data with a password sent from a terminal via the network, fetches and outputs the corresponding stored data in response to the direct input of the password into the shared output device.

[Industrial Applicability]

The present invention relates to a shared output device having a security function, which outputs data from the shared output device connected to a network while keeping security. The tendency of computers toward networking has recently been remarkable, and it is now a common practice to manage a high-function/high-performance output device by sharing by a plurality of terminals. Under these circumstances, when printing a document not to be perused by

others by use of an output device, there is a demand for ensuring security.

[Problems to be Solved by the Invention]

It is conventionally the general practice to arrange a high-function/high-performance output device 23 connected to a common control unit 22 via a network from a plurality of terminals 21 at a physically remote place. Printing a confidential document from a terminal 21 by the use of the output device 23 installed at such a remote place poses the problem of difficulty to ensure security.

It is an object of the present invention to once store data with a password sent via a network without outputting, into a memory of the shared output device, output the data in response to the input of the password or the like, and securely output the confidential data by using the shared output device.

[Means for Solving the Problem]

Fig. 1 illustrates the configuration of the principle of the present invention.

In Fig. 1, a terminal 1 performs various steps of processing in connection with a network.

The shared output device 2 is connected to the network, receives data with a password (or a password and a print ID)

sent from any of the terminals 1, once stores the data, directly fetches the corresponding data stored in the memory in response to input of the password (or the password and the print ID) and outputs the data.

[Operation]

In the present invention, as shown in Fig. 1, the shared output device 2 receives data with a password (or a password and a print ID) sent from the terminal 1 via the network, once stores the data in the memory, directly fetches the corresponding data stored in the memory in response to input of the password (or the password and the print ID) and outputs the data.

Therefore, by once storing the data with a password sent via the network in the memory in the shared output device 2, without outputting the data, and outputting the data in response to input of the password or the like, it is possible to safely output the confidential data by means of the shared output device.

[Embodiments]

The configuration and operation of an embodiment of the present invention will be sequentially described in detail with reference to Figs. 1 to 5.

In Fig. 1, the terminal 1 is connected to a network

(such as a LAN) to carry out various steps of processing.

The shared output device 2 comprises a shared control unit 3 conducting various controls for sharing the output device 5 via the network, an auxiliary memory 4 storing data, an output unit 5 outputting the data requested by the terminal via the network, and a password input unit 6 inputting a password, a print ID and the like.

Fig. 2 is a configuration diagram of the shared output device of the present invention.

In Fig. 2, the imaging control unit 7 develops data sent from the terminal 1 via the network into an image and stores the image in a memory 8.

The memory 8 temporarily stores image data.

A security control unit 9 fetches the corresponding image data from the auxiliary memory 4 in response to input of a password or a print ID from a password input unit 6, sends the data to the output device 5 to cause it to output the data.

The receiving operation of data from the terminal 1 in the configuration shown in Figs. 1 and 2 will now be described in detail with reference to the flowchart shown in Fig. 3.

In Fig. 3, at (11), the shared output device receives a printing job, performs an exclusive control of the printer (output device), and sends data to the imaging control unit

7. The shared control unit 3 exclusively receives data (printing job) sent from the terminal 1 via the network in Figs. 1 and 2, for example, accepts only data received first, and sends the accepted data to the imaging control unit 7.

In step (12), data for a page is taken up from the print data, and stores it in the memory. That is, data for a page is taken up from the data sent from the shared control unit 3 by an imaging control unit shown in Fig. 2, which develops the data into an image and stores it in the memory 8.

At (13), it is determined whether or not the data has a password. If YES (for example, in the case of data with a password shown in Fig. 5), the image data of the memory 8 is stored in the auxiliary memory 4 at (14). In the case of NO, on the other hand, the image data of the memory 8 is sent to the output device in step (15), and a page is outputted.

Step (16) covers initialization. This step initializes the areas which have sent data from the memory 8 to the auxiliary memory 4 or the output device 5 in steps (14) and (15).

At (17), it is determined whether or not the print job has come to an end. If YES, step (18) is executed. If NO, (20) and subsequent steps are repeated.

When using the auxiliary memory, step (18) stores the print ID and the password. As shown to the right in Fig. 3,

when data with a password is stored in the auxiliary memory 4, the printer (address) of image data is registered in the management table 10 in correlation with the print ID and the password, to prepare for outputting.

As a result of the above-mentioned steps of processing, data is stored in the auxiliary memory 4 when the data sent from the terminal 1 to the shared output device 2 via the network has a password, and the data is outputted for printing or the like by the output device when the data has no password.

The operation of inputting and outputting into and from the shared output device 2 in the configuration shown in Figs. 1 and 2 will now be described in detail with reference to the flowchart shown in Fig. 4.

In Fig. 4, a password and a print ID are entered at (21). A password input unit 6 shown in Figs. 1 and 2 receives input of a password and a print ID from, for example, the keyboard, and an output instruction is given.

At (22), the security control unit 9 retrieves the data of the password and the print ID stored in the auxiliary memory 4.

Step (23) determines whether or not data is present. In case of YES, the (24) and subsequent steps are performed. If NO, which means that image data is not stored in correlation with a password or a print ID, the step comes to

an end (END).

In step (24), the end of the operation "in printing" is waited for.

Step (25) fetches individual page data of the print job corresponding to the print ID by means of the auxiliary memory 4, and sends them to the output device 5.

At (26), the output device 5 conducts output (printing).

As a result of these steps, when corresponding image data is stored in the auxiliary memory 4 in response to input of a password and a print ID directly from the password input unit 6 and an output instruction given thereto upon a visit by the first user of the terminal 1 to the place of the shared output device 2, it becomes possible to cause safe printing of a confidential document by fetching and sending it to the output device 5.

Fig. 5 illustrates an example of data with a password of the present invention. This is an example of data in a case where data is sent from the terminal 1 to the shared control unit 3 via the network. When the data is confidential, data is sent by setting a password or a print ID. As a result, the data sent by YES in step (13) and step (14) in Fig. 3 is stored in the auxiliary memory 4 without being outputted. The data is outputted by the processing shown in the flowchart of Fig. 4. When the data is not confidential, on the other hand, the data is sent without

setting a password or a print ID. The data is thus outputted from the output device 5 upon NO in step (13) and (15) shown in Fig. 3.

[Advantages]

According to the present invention, as described above, the adopted configuration is such that data with a password sent from the terminal 1 to the shared output device 2 with the network is once stored, and the corresponding data is outputted in response to the password or the like. It is thus possible to safely output confidential data by use of the shared output device connected to the network.

4. Brief description of the Drawings

Fig. 1 is a principle configuration view of the present invention; Fig. 2 is a configuration view of the shared output device of the present invention; Figs. 3 and 4 are flowcharts for illustrating the operation of the present invention; Fig. 5 illustrates an example of data with a password of the present invention; and Fig. 6 is a descriptive view of the conventional art.

In the drawings, 1: terminal, 2: shared output device, 3: shared control unit, 4: auxiliary memory, 5: output device, 6: password input unit, 7: imaging control unit, 8: security control unit, and 10: control table.

Patent Applicant: Fujitsu Limited

Agent: Patent Attorney, Morihiro OKADA

FIG. 1

(1) NETWORK

(2) TERMINAL

(3) TERMINAL

3: SHARED CONTROL UNIT

4: AUXILIARY MEMORY

5: OUTPUT DEVICE

6: PASSWORD INPUT DEVICE

2: SHARED OUTPUT DEVICE

PRINCIPLE CONFIGURATION VIEW OF INVENTION

FIG. 2

(2) NETWORK

8: MEMORY

3: SHARED CONTROL UNIT

7: IMAGING CONTROL UNIT

5: OUTPUT DEVICE

6: PASSWORD INPUT UNIT

9: SECURITY CONTROL UNIT

4: AUXILIARY MEMORY

CONFIGURATION VIEW OF SHARED OUTPUT DEVICE OF INVENTION

FIG. 3

(11) THE SHARED CONTROL UNIT RECEIVES PRINT JOB, PERFORMS EXCLUSIVE CONTROL OF PRINTER, AND SENDS PRINT DATA TO

IMAGING CONROL UNIT

(12) DATA FOR 1 PAGE IS FETCHED FROM PRINT DATA AND STORED IN MEMORY

(13) DOES DATA HAVE PASSWORD?

(14) MEMORY DATA IS STORED IN AUXILIARY MEMORY

(15) DATA IS SENT TO OUTPUT DEVICE AND DATA FOR 1 PAGE IS OUTPUTTED

(16) INITIALIZATION OF MEMORY

(17) END OF PRINT JOB?

(18) WHEN USING AUXILIARY MEMORY, PRINT ID AND PASSWORD ARE STORED

10: CONTROL TABLE

PRINT ID

PASSWORD

IMAGE DATA POINTER

FLOWCHART FOR ILLUSTRATING OPERATION OF INVENTION (UPON RECEIVING)

FIG. 4

(21) INPUT PASSWORD AND PRINT ID

(22) SECURITY CONTROL UNIT RETRIEVES CORRESPONDING DATA OF PASSWORD AND PRINT ID STORED IN AUXILIARY MEMORY

(23) DATA IS PRESENT

(24) END OF PRINTING OPERATION IS CURRENTLY WAITED FOR

(25) INDIVIDUAL PAGE DATA OF PRINT JOB CORRESPONDING TO

PRINT ID ARE SENT FROM AUXILIARY MEMORY TO OUTPUT DEVICE

(26) OUTPUT

FLOWCHART FOR ILLUSTRATING OPERATION OF INVENTION (UPON OUTPUTTING)

FIG. 5

(1) HEADER

(2) PRINT ID

(3) PASSWORD

(4) DATA

EXAMPLE OF DATA WITH PASSWORD OF INVENTION

FIG. 6

(1) NETWORK

21: TERMINAL

21: TERMINAL

22: SHARED CONTROL UNIT

23: OUTPUT DEVICE

DESCRIPTIVE VIEW OF CONVENTIONAL ART

⑲日本国特許庁（JP）　⑪特許出願公開

⑫公開特許公報（A）　平3－269756

⑤1Int. Cl.⁵	識別記号	庁内整理番号
G 06 F 15/00	330 A	7218－5L
13/00	354 D	7459－5B

⑬公開　平成3年(1991)12月2日

審査請求　未請求　請求項の数 1　（全5頁）

⑤4発明の名称　セキュリテイ機能付共用出力装置

⑳特　願　平2－70614
㉒出　願　平2(1990)3月20日

⑦2発明者　石黒　敬二　神奈川県川崎市中原区上小田中1015番地　富士通株式会社内
⑦1出願人　富士通株式会社　神奈川県川崎市中原区上小田中1015番地
⑦4代理人　弁理士　岡田　守弘

明　細　書

1．発明の名称

セキュリティ機能付共用出力装置

2．特許請求の範囲

ネットワークに接続された共用出力装置から機密性を保持して出力するセキュリティ機能付共用出力装置において、

端末(1)からネットワークを介して送られてきた暗証番号付きのデータを共用出力装置(2)が受信して一旦保存し、当該共用出力装置(2)に直接に暗証番号が入力されたことに対応して保存しておいた該当するデータを取り出して出力するように構成したことを特徴とするセキュリティ機能付共用出力装置。

3．発明の詳細な説明

〔概要〕

ネットワークに接続された共用出力装置から機密性を保持して出力するセキュリティ機能付共用出力装置に関し、

ネットワークを介して送られてきた暗証番号付きのデータを出力することなく共用出力装置内のメモリに一旦保存し、暗証番号などの入力に対応して出力し、共用出力装置を用いて機密性のあるデータを安全に出力することを目的とし、

端末からネットワークを介して送られてきた暗証番号付きのデータを共用出力装置が受信して一旦保存し、当該共用出力装置に直接に暗証番号が入力されたことに対応して保存しておいた該当するデータを取り出して出力するように構成する。

〔産業上の利用分野〕

本発明は、ネットワークに接続された共用出力装置から機密性を保持して出力するセキュリティ機能付共用出力装置に関するものである。近年、コンピュータのネットワーク化が進み、高機能／高性能の出力装置を複数の端末から共用して運用することが行われている。この際、出力装置を用

いて他人に見せたくない書類を印刷などする場合、機密保護を行うことが望まれている。

〔従来の技術と発明が解決しようとする課題〕

従来、第6図に示すように、複数の端末21からネットワークを介して共用制御装置22に接続した高機能／高性能の出力装置23を物理的に離れた場所に置くことが多い。この離れた場所に配置した出力装置23を用い、端末21から機密性のある印刷物を印刷する場合、機密保護を図り難いという問題があった。

本発明は、ネットワークを介して送られてきた暗証番号付きのデータを出力することなく共用出力装置内のメモリに一旦保存し、暗証番号などの入力に対応して出力し、共用出力装置を用いて機密性のあるデータを安全に出力することを目的としている。

〔課題を解決する手段〕

第1図は、本発明の原理構成図を示す。

第1図において、端末1は、ネットワークに接続して各種処理を行う端末である。

共用出力装置2は、ネットワークに接続し、いずれかの端末1から送られてきた暗証番号（あるいは暗証番号とプリントＩＤ）付きのデータを受信してメモリに一旦保存し、当該共用出力装置2に直接に暗証番号（あるいは暗証番号とプリントＩＤ）の入力に対応してメモリに保存しておいた該当するデータを取り出して出力するものである。

〔作用〕

本発明は、第1図に示すように、端末1からネットワークを介して送られてきた暗証番号（あるいは暗証番号とプリントＩＤ）付きのデータを共用出力装置2が受信してメモリに一旦保存し、当該共用出力装置2に直接に暗証番号（あるいは暗証番号とプリントＩＤ）の入力に対応してメモリに保存しておいた該当するデータを取り出して出力するようにしている。

従って、ネットワークを介して送られてきた暗証番号付きのデータを出力することなく共用出力装置2内のメモリに一旦保存し、暗証番号などの入力に対応して出力することにより、共用出力装置2を用いて機密性のあるデータを安全に出力することが可能となる。

〔実施例〕

次に、第1図から第5図を用いて本発明の1実施例の構成および動作を順次詳細に説明する。

第1図において、端末1は、ネットワーク（例えばＬＡＮ）に接続して各種処理を行う端末である。

共用出力装置2は、ネットワークを介して出力装置5を共用するための各種制御を行う共用制御装置3、データを保存する補助記憶装置4、端末からネットワークを介して依頼を受けたデータを出力する出力装置5、暗証番号、プリントＩＤなどを入力する暗証番号入力装置6から構成されるものである。

第2図は、本発明に係る共用出力装置の構成図を示す。

第2図において、イメージ化制御部7は、端末1からネットワークを介して送られてきたデータをイメージに展開してメモリ8に格納するものである。

メモリ8は、イメージデータを一時的に格納するものである。

セキュリティ制御部9は、暗証番号入力装置6からの暗証番号、プリントＩＤの入力に対応して、該当するイメージデータを補助記憶装置4から取り出して出力装置5に送り、出力させるものである。

次に、第3図フローチャートを用いて第1図、第2図構成における端末1からのデータの受け付けの動作を詳細に説明する。

第3図において、①は、共用制御装置がプリントジョブを受け付け、プリンタ（出力装置）の排他制御を行い、プリントデータをイメージ化制御部7に送る。これは、第1図、第2図で端末1からネットワークを介して送られてきたデータ（プ

リントジョブ）を共用制御装置3が排他的に受け付け、例えば最も遠く受信したデータのみを受け付け、この受け付けデータをイメージ化制御部7に送る。

⑫は、プリントデータから1ページ分を取り出し、メモリへ格納する。これは、第2図イメージ化制御部7が共用制御装置3から送られてきたデータのうちから1ページ分を取り出し、イメージデータに展開してメモリ8に格納する。

⑬は、暗証番号付きか否かを判別する。ＹＥＳの場合（例えば第5図暗証番号付きのデータの場合）には、⑭で補助記憶装置4へメモリ8のイメージデータを保存する。一方、ＮＯの場合には、⑮でメモリ8のイメージデータを出力装置へ送り、1ページを出力する。

⑯は、初期化を行う。これは、⑭、⑮でメモリ8から補助記憶装置4あるいは出力装置5に送った領域を初期化する。

⑰は、プリントジョブの終了か否かを判別する。ＹＥＳの場合には、⑱を行う。ＮＯの場合には、⑫以降を繰り返し行う。

⑱は、補助記憶装置を使用した場合には、プリントＩＤ、暗証番号を保存する。これは、右側に示すように、⑬ＹＥＳ、⑭で、暗証番号付きのデータとして補助記憶装置4に保存した場合に、プリントＩＤ、暗証番号に対応づけてイメージデータのポインタ（アドレス）を管理テーブル10に登録し、出力時に備える。

以上の処理によって、端末1からネットワークを介して共用出力装置2に送られてきたデータが暗証番号付きのデータのときに補助記憶装置4に保存し、一方、暗証番号付きでないデータのときに出力装置5によって印刷などするようにしている。

第4図フローチャートを用いて第1図、第2図構成における共用出力装置2へ暗証番号を入力して出力する動作を詳細に説明する。

第4図において、⑳は、暗証番号、プリントＩＤを入力する。これは、第1図、第2図暗証番号入力装置6、例えばキーボードから暗証番号、プリントＩＤを入力して出力指示を与える。

㉑は、セキュリティ制御部9が補助記憶装置4に保存されている該当暗証番号、プリントＩＤのデータを検索する。

㉒は、データありか否かを判別する。ＹＥＳの場合には、㉓以降を行う。ＮＯの場合には、暗証番号、プリントＩＤに対応づけてイメージデータが保存されていなかったので、終了する（ＥＮＤ）。

㉓は、現在、印刷中の終了を待つ。

㉔は、補助記憶装置4より、プリントＩＤに対応するプリントジョブの各ページデータを取り出して出力装置5に送る。

㉕は、出力装置5が出力（印刷）する。

以上の処理によって、端末1の利用者が共用出力装置2の場所に出掛けて直接に暗証番号入力装置6から暗証番号、プリントＩＤを入力して出力指示を与えたことに対応して、補助記憶装置4に該当するイメージデータが保存されていたときにこれを取り出して出力装置5に送って印刷などすることにより、秘密性の文書を安全に印刷などさせることが可能となる。

第5図は、本発明に係る暗証番号付のデータ例を示す。これは、端末1からネットワークを介して共用制御装置3に送るデータ例を示す。機密性の場合には、暗証番号、プリントＩＤなどを設定したデータを送る。これにより、第3図⑬ＹＥＳ、⑭で送ったデータが出力されることなく補助記憶装置4に保存される。そして、第4図フローチャートに示す処理によって出力される。一方、機密性でない場合には、暗証番号、プリントＩＤなどを設定しないままのデータを送る。これにより、第3図⑬ＮＯ、⑮によって出力装置5から出力される。

〔発明の効果〕

以上説明したように、本発明によれば、端末1からネットワークを介して共用出力装置2に送られてきた暗証番号付きのデータを一旦保存し、暗証番号などの入力に対応して該当するデータを出

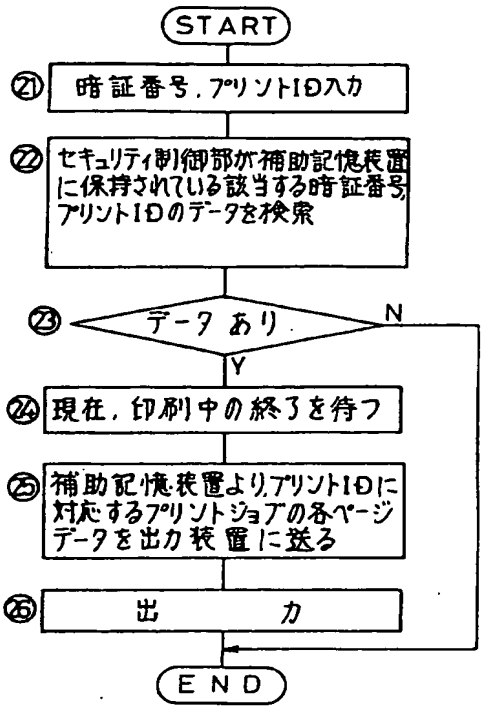
力する構成を採用しているため、ネットワークに接続された共用出力装置2を用いて機密性のあるデータを安全に出力することができる。

4．図面の簡単な説明

第1図は本発明の原理構成図、第2図は本発明に係る共用出力装置の構成図、第3図、第4図は本発明の動作説明フローチャート、第5図は本発明に係る暗証番号付のデータ例、第6図は従来技術の説明図を示す。

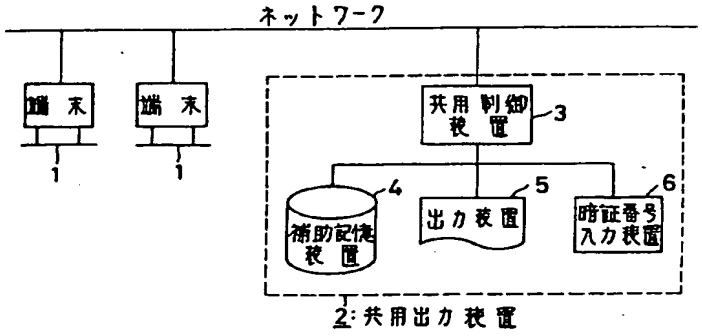
図中、1は端末、2は共用出力装置、3は共用制御装置、4は補助記憶装置、5は出力装置、6は暗証番号入力装置、7はイメージ化制御部、8はセキュリティ制御部、10は管理テーブルを表す。

特許出願人　富士通株式会社
代理人弁理士　岡田　守弘



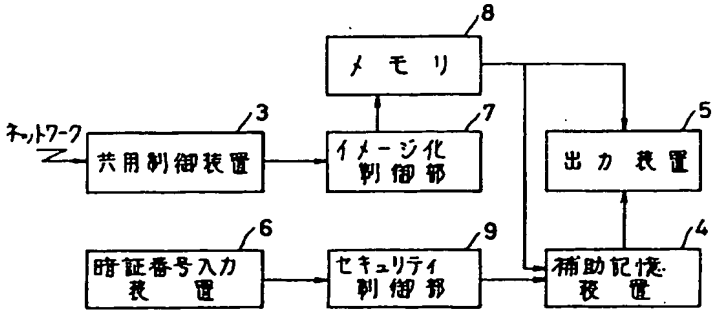
本発明の動作説明フローチャート(出力時)

第　4　図



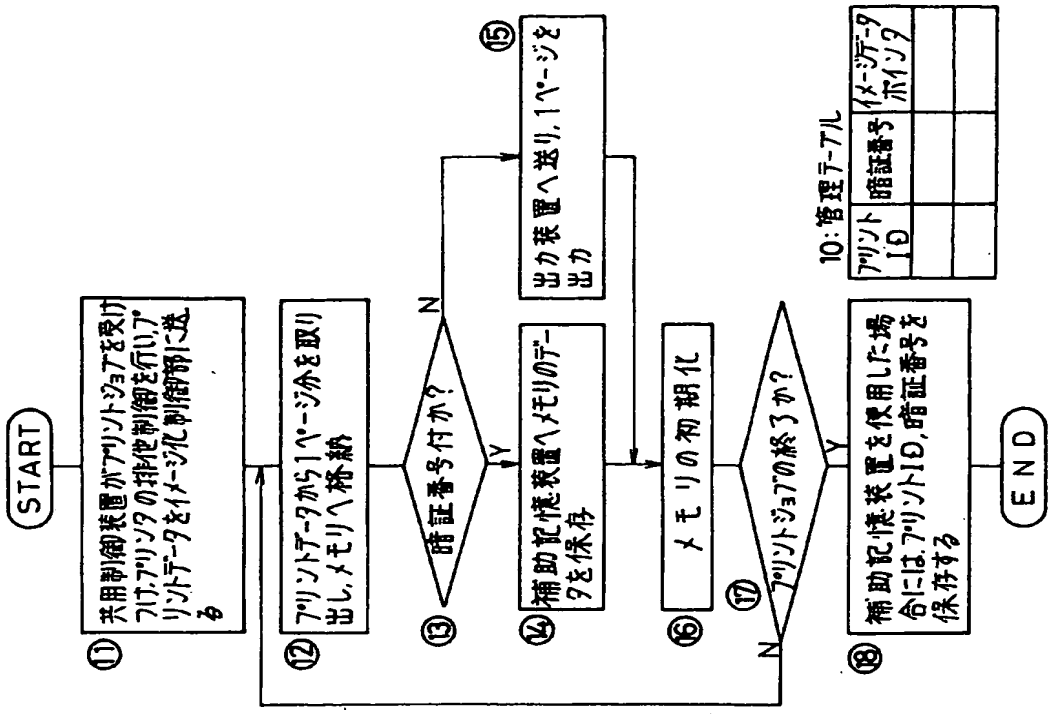
本発明の原理構成図

第　1　図



本発明に係る共用出力装置の構成図

第　2　図



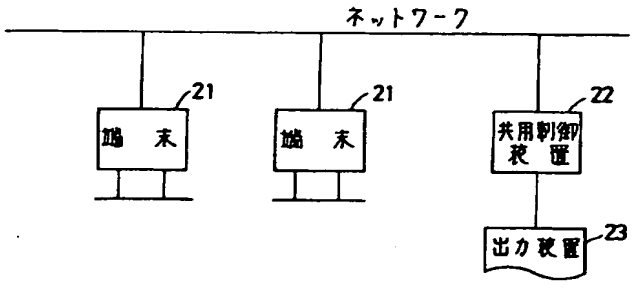
本発明の動作説明フローチャート(受付け時)

第 3 図

ヘッダ	プリントID	暗証番号	データ

本発明に係る暗証番号付のデータ例

第 5 図



従来技術の説明図

第 6 図